CYBER SECURITY HUB

CYBER SECURITY STANDARDS AND FRAMEWORKS

Assessment And Effective Communication Of Enterprise Risk

Sponsored by

ENZOIC

Market Report

Table Of Contents

Executive Summary

No organization will ever be able to prevent 100 percent of cyber-attacks, but through careful due diligence, it's possible to competitively outpace the threat with early detection and powerful response tactics.

This market report serves to educate and inform business leaders – encompassing private enterprise, government agencies, and non-profits – about the need for a prioritized, flexible, repeatable, performance-based, and cost-effective standards-based framework for critical infrastructure cyber security.

With that plan in hand, security leaders can achieve broad organizational buy-in to assist with planning for an effective implementation and promote the notion that, "Cyber security is everyone's job."

Creating Business Value With Cyber Security Standards And Frameworks

Many organizations must comply with a mixture of state-mandated, industry-specific and international cyber security regulations. The challenge for an organization operating nationally, or even globally, is considerable.

According to survey results, the majority of enterprise organizations in the U.S. tackle this issue with the help of one or more security frameworks. The majority of respondents in our annual benchmark of enterprise cyber security trends and predictions utilize the NIST CSF framework (53%). More than 45% said they use the ISO/IEC 27001/27002 (46%). CIS Critical Security Controls (36%) were also a popular response.

Compared to the most recent market assessment we conducted, the ISO 27001 adoption remained consistent while NIST CSF usage increased from nearly 40% to 53%. CIS Critical Security Controls and PCI DSS usage also remained at similar levels of adoption from our previous mid-year survey to the end-of-year results.

Somewhat surprising is that 15% of respondents say their organization is not using any type of security framework, though this is down from nearly 30% of respondents only 6 months earlier.

Additional responses included more ISO/IEC standards, COBIT5, Mitre ATT&CK and even proprietary frameworks.

A framework provides a common language and systematic methodology for managing cyber security risk. A framework is designed to complement, not replace, an organization's cyber security program and risk management processes. It provides a gap analysis tool for existing enterprise cyber security programs. A framework may be used as an overlay tool for existing programs or it can serve as a model for establishing new cyber security programs.

One benefit of using a framework is to tailor activities to any organization's needs. It can be carried out and adhered to in many different systems – with the aim of limiting threats and improving an organization's risk management abilities. Frameworks are technology neutral and can be implemented on several levels, including IT, cyber-physical systems and interconnected devices (more commonly known as IoT).

Industry Regulation As A Guidepost For Popular Frameworks

The enterprise cyber security industry has immediate and on-going needs for prioritized, flexible, repeatable, performance-based and cost-effective standards-based frameworks.

Regulated industries, such as banking, financial services and insurance (BFSI) are often associated with a high level of framework adoption. In contrast, the U.S. healthcare regulation (HIPAA) does not inherently offer standards or a framework; relying on external industry best practices.

Most industry sectors are under-regulated and therefore adopt cyber security standards and industry frameworks to build their own gap analysis and prioritization of vulnerabilities. "Regardless of industry, common objectives exist such as managing risk, securing data or protecting intellectual property," said data privacy and cyber security law expert Jamal Hartenstein. "Enterprises aren't regulated on the latter, but laws are in place to protect consumer information, and many of those laws point to the same common standards and frameworks."

"Regardless of industry, common objectives exist such as managing risk, securing data or protecting intellectual property."

Jamal Hartenstein
Data Privacy and Cyber Security Law Expert

A variety of standards and frameworks exist today, including:

HIPAA/HITECH:
The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in August 1996, and was updated by the HIPAA Privacy Rule in 2003 and the HIPAA Security Rule in 2005. The Health Information Technology for Economic and Clinical Health (HITECH) Act changed HIPAA and introduces obligations for information security to demonstrate compliance.

Cyber Security Role:
If your organization is collecting personal health information (PHI), security controls are necessary to ensure that it remains secure.

Industry Regulation As A Guidepost For Popular Frameworks

PCI DSS:

The Payment Card Industry Data Security Standard (PCI DSS) is a security standard used to securely transfer payment card data. Conforming to the standard can give customers more confidence in the organization's ability to protect its data. Additionally, PCI-DSS compliance better prepares an organization to comply with overlapping requirements of standards and frameworks, such as COBIT or HIPAA.

Cyber Security Role:

Specific areas of enforcement and controls are based on the PCI DSS level, but could include self-assessment security questionnaires, periodic network scans and 3rd party security audits to demonstrate compliance with the standard.

NIST:

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. The NIST Cybersecurity Framework (CSF) helps businesses of all sizes better understand, manage, and reduce their cyber security risk and protect their networks and data. The Framework is voluntary and gives organizations an outline of best practices to help decide where to focus time, funding and resources for cyber security protection. The Framework provides five focal areas: Identify, Protect, Detect, Respond, and Recover.

Cyber Security Role:

Cyber security professionals will likely lead the identification, definition and enforcement of security controls governed by the Framework.

ISO/IEC 27000:

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27000 family of standards helps organizations manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). An ISMS is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Cyber Security Role:

An organization may use this family of standards to enhance & report on security management practices.

Center for Internet Security:
The Center for Internet Security (CIS) is a non-profit entity focused on safeguarding private and public organizations against cyber threats. The CIS Controls are a standard and series of best practices for securing IT systems and data against pervasive cyber-attacks. The 20 CIS Controls (originally known as the SANS Top 20) are segmented into basic, foundational and organizational. Additional resources are available including risk assessment tools. The guidelines are continuously refined and verified by a volunteer community of IT professionals.

Cyber Security Role:
The 20 CIS Controls outline what organizations should do as their first steps in cyber security. They have been proven to mitigate 85 percent of the most common vulnerabilities and can be utilized in conjunction with the NIST CSF.

"The Mitre ATT&CK framework is not as well known in the cyber security industry as CIS CSC or NIST CSF, but it should be on the radar of IT security leaders because of its utility and thoroughness in its approach to safeguarding an enterprise," said Hartenstein.

Regardless of the path chosen, security professionals must remain aware of the ongoing changes to frameworks and specific requirements that are relevant to their industry. For example, when NIST last revised its Special Publication 800-63-B on Authentication and Lifecycle Management, previous recommendations for handling of passwords were abandoned. They reversed previous guidance around password complexity rules in favor of screening passwords against a corpus of compromised passwords from previous data breaches.

Security professionals that failed to keep current with change have had to jump to reassess their security controls and processes. By keeping an eye on the standards development organization, security professionals can evaluate new changes being reviewed before they are finalized and prepare their organizations accordingly.

Assessing The Organization's Cyber Security Readiness

While the framework does not mandate how the organization achieves the outcomes, one way to approach the process is to develop a current-state profile of organizational practices against the subcategories of the framework.

"A major benefit from using a framework is to support better decision-making and help deliver consistent outcomes," said IBRS cyber security analyst James Turner. "When it comes to security and risk, a framework is only as useful as the intellectual effort required to understand the framework and how it applies to an organization's risks."

Along with mission objectives and operating methodologies, the organization can utilize the current-state profile to create a gap analysis and a prioritized action plan. The priority, size of gap, and estimated cost of the corrective actions help organizations plan and budget for cyber security improvement activities.

Organizations that formally adopt and can demonstrate compliance with cyber standards establish differentiation from competitors in their industry who cannot. Using third-party auditing can provide another way to formalize and differentiate the organization's security commitment.

> "A major benefit from using a framework is to support better decision-making and help deliver consistent outcomes"
>
> **James Turner**
> Cyber Security Analyst, IBRS

Industry Approaches To The Use Of Frameworks

"HIPAA is the main compliance driver for healthcare," says Randall Frietzsche, enterprise CISO for Denver Health. HIPAA points to NIST for details on how to determine conformance. "Talking to committees and the board about encryption and firewalls doesn't mean much to them, but when I can explain this is what HIPAA says or the government requires, it provides a level-set about protecting the organization and detecting threats. All areas of our strategy are aligned with the frameworks and programs of the team." As a technical leader, Frietzsche uses a framework to provide specifics to the security team about guidance for pursuing it with mappings to multiple technical sources. Even if HIPAA were not the driver, Frietzsche says a compliance framework would have been used to build an appropriate structure for the security program.

The Health Information Trust Alliance, or HITRUST, is a privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework that can be used by organizations that create, access, store or exchange data. "The HITRUST controls framework is widely adopted in the healthcare industry," said IT and healthcare CISO Rebecca Wynn. The organization has released a single framework assessment that includes the controls necessary to address the NIST CSF requirements and an addendum to the HITRUST CSF Assessment report has been added to display the HITRUST CSF controls through the lens of the NIST CSF Core Subcategories.

"There are many challenges working with self-owned data as well as with third parties on how to secure it," said Glenda Lopez, Director of Global Risk and Compliance with The Henry M. Jackson Foundation for the Advancement of Military Medicine. The Foundation's mission is healthcare research and at the same time is a non-profit organization and U.S. Department of Defense contractor. "With personnel overseas, we encounter GDPR implications and how to secure information in the field and educating them on how it is brought back keeping the right security controls in place."

Universities, by their nature, are open networks. "We cannot assume the network is safe," said Randy Marchany, CISO for university Virginia Tech. "Organizationally, we need to have a policy stating what frameworks the organization will follow. I need a data classification set of policies and standards that declares what is high-risk data, etc. And then you need a standard that describes the minimum security standards declared." In some organizations, policy and standards information has always been there, but having separate end-point and server teams, for example, it may not all reside together in one place. Also, different departments have specific requirements, such as laws requiring HR to report breaches.

Where To Start Your Journey

Security leaders should align the implementation to their specific business processes and situations. It is tempting to take a security framework and try to turn it directly into an operational guide, but this is ill-advised. While all the security practices may have a place, it's essential to make a proper consideration of the risk and apply a balanced approach that doesn't add excessive friction to the process.

Standards and frameworks are generally established using norms by industry. Expectations for compliance then tend to roll down the supply chain. Once an organization establishes a cyber standard or framework, considerable investments are made to establish compliance with less investment required for maintenance. Therefore, switching costs can be high.

The current-state assessment is a starting point to document where the security controls stand today. From there, an organization can keep going through controls to understand where there is strength and where gaps exist.

EXISTING PROGRAM INTEGRATION

- Compare your current program to the cyber security framework in order to identify opportunities for improvement.
- Incorporate framework elements not already advdressed in the current program.
- Global Risk Director Glenda Lopez suggested, "Prioritize the information and identify what is going to give the highest protection as well as the budgetary needs."

ESTABLISHING A NEW PROGRAM

- Use a cyber security framework as a model to start a new program.
- Develop a high-level strategy for meeting each functional objective.
- How does the organization envision implementation?
- Will it use internal or contracted resources? Manual or automated processes?
- How will the function be managed?
- What is the required implementation timeline?
- What general tools, systems, or service agreements will be required?

In all cases, the proper framework use requires that companies view it as a collection of potential "outcomes" to achieve rather than a checklist of "actions" to perform. In other words, the framework's core outlines the objectives a company may wish to pursue, while providing flexibility in terms of how, and even whether, to accomplish them.

There definitely are areas of a framework that do not apply to every organization. Think about the framework as a baseline to build from. In email, for example, there are some technology enhancements to control phishing emails or "sinkholing" a domain from coming through. That control is needed, but it may not be part of the framework. Organizations have the flexibility to select as well as go above and beyond.

The starting point is really a mapping of the controls to what the organization currently has in place. The organization can then address areas where no controls are in place or there are too many unnecessary or less effective controls. The mapping must be done with process owners and not in isolation. There are also companies that will provide a service by benchmarking an organization's controls.

At the University of Wisconsin-Madison, the cyber security team built a spreadsheet – dubbed The Crosswalk – that enables a side-by-side baseline comparison of controls from multiple frameworks. Like a visual gap analysis, "it makes it easy to spot where the deltas are," said CISO Bob Turner. However, even this alignment may not provide all of the answers. "You may find yourself creating controls where there is nothing applicable."

> "You may find yourself creating controls where there is nothing applicable."
>
> **Bob Turner**
> CISO, University of Wisconsin-Madison

Understanding An Organization's True Risk

What is the true risk of that server in your network? What applications are running on it? What ports and systems are open? Who has access? Where does it sit within the network?

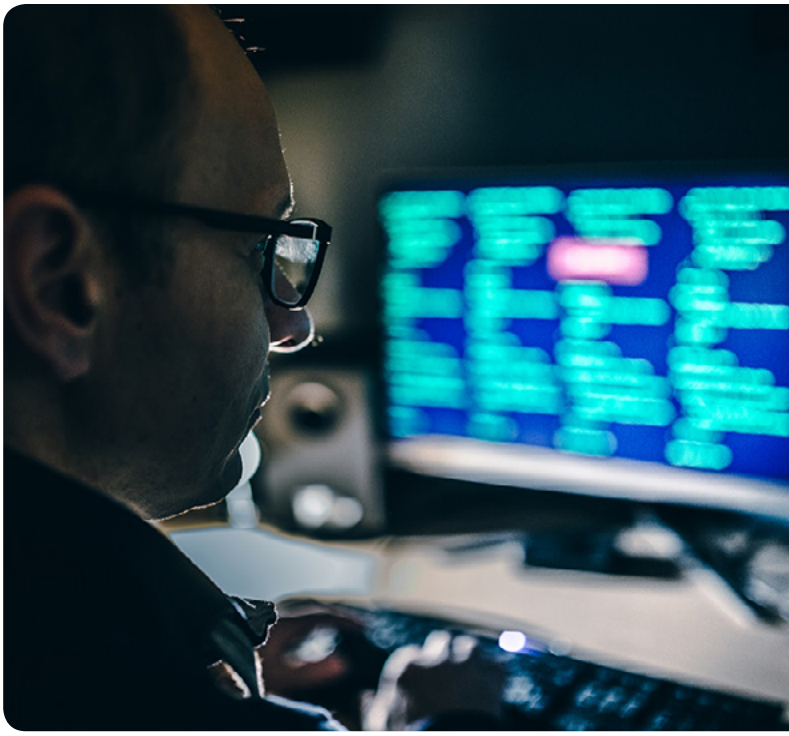
Risk is more than just what patches haven't been applied. What are the true risks of not applying them? What is the true risk of having that port open or that service running? What is the true risk of having that server sitting where it is in the environment? Etc.

"CISOs need to be business enablers," said Turner. "Really listen to the business and try to move towards a framework or set of standards that help get the business ahead; hopefully not injure the business at all." Turner cautioned about assessing only the upside of a framework and that security leaders need to similarly understand the business impact from non-compliance to industry, regulatory or partner requirements.

There are a lot of security tools to choose from noted Lopez. "A risk assessment prioritizes the benefit and impact to the organization. You can then weigh this against the cost of a data breach. And you can compare the value to cost of a breach."

In the U.S., the NIST Cybersecurity Framework is widely pointed as the go-to standard for security practices and development. The FTC, SEC, state legislators, and others are increasingly using language requiring "reasonable" safeguards. According to Tara Swaminatha, a data privacy and cyber security partner at Squire Patton Boggs in Washington, D.C., and former federal prosecutor in the Computer Crime & Intellectual Property Section at the U.S. Department of Justice, organizations having developed a cyber security program following NIST CSF v1.1 will mitigate cyber security-related liability exposure in the face of regulatory enforcement actions.

"Under current law in the United States, businesses have no clear guidance about how to build a security program that would comply with the law," wrote Swaminatha. "No matter what security protections a business employs, it cannot be certain that the protections would be judged as being sufficient in a lawsuit or regulatory investigation." In many areas of the law, negligence standards tend to be much clearer and businesses generally know they can be considered legally sufficient if certain standards or conditions are met. In other words, those standards instruct businesses adequately on the steps to take to be reasonable and not negligent.



Government Agency Mandate Signals Supply Chain Evolution

Beyond the enterprise uptake of cyber security frameworks, the U.S. government mandated adoption of the NIST CSF in the public sector via Executive Order in 2018. This could lead to a requirement where suppliers for an agency or government-funded entity (such as a University or Healthcare system) will need to document and demonstrate capability to conform to the NIST framework.

"In the healthcare industry, we are already seeing that," said Wynn. "Some big associations such as Blue Cross Blue Shield Association want their vendors to be HITRUST CSF certified along with having a SOC 2 Type 2 attestation. With all the data breaches we hear about daily, individuals who buy your product or service and companies who do business with you or through you want assurances that you do take security, privacy, compliance, and risk management seriously. NIST CSF is one way to do that."

"Definitely. Third-party breaches are huge," remarked Lopez. "We need a knowledge of who we're working with and each entity is assessed during an on-boarding process. If they're dealing with sensitive information, we document any gap they have. Then a decision is needed on how to engage; also, it's an opportunity for them to be re-assessed on those gaps. Fourth-party relationships become a risk too. For non-sensitive information, we will assess annually but re-assess if that relationship changes. I am seeing a need for working with similar controls and working at a similar level of readiness across organizations. We're only as strong as the weakest link in the chain."

"As a university receiving federal grants, we must make sure that university standards meet the needs of the federal requirements," said Marchany. "Pressure will come when the U.S. Department of Education suggests that tools use the NIST SP 800-171 standard."

To work with government, Amazon had to create a FedRAMP cloud separate from its commercial cloud services that specifically meets the NIST 800-171 standard. For universities, especially those receiving grant money, it will become an issue. There will be service level agreements set, but it may require an agreement on a specific contractual requirement to utilize a specific framework.

Cyber Security Framework SWOT Analysis

For the longest time, IT has been considered a cost to business. “When working with business leaders across the company, security needs to be viewed by how it provides a competitive advantage to the company’s success,” said former food supply chain CISO Mike Welch. “Aligning security with the business goals allows the business to achieve its goals while protecting the brand.”

Organizations can utilize the cyber security framework as a business differentiator. Higher education CISO Turner likens the opportunity to an RFI process. “You know there is alignment when working with the U.S. federal government, for example, and this streamlines the process of creating the business relationship as well as building confidence in achieving the goal, whether it be funding, partnership, or otherwise.”

A technique for identifying risk and adoption factors of a framework is to evaluate its perceived strengths, weaknesses, opportunities, & threats (or SWOT analysis).

STRENGTHS

- It is concise, efficient, and adaptable.
- It comes at cyber security from the point of view of risks rather than just suggesting controls to implement.
- A tiered approach, with their multi-level measurement, are an improvement over the usual binary yes/no method to cyber security evaluation.

WEAKNESSES

- By complying, organizations are assumed to have less risk; however, a framework doesn’t measure risk.
- A framework does not show the return on investment (ROI) of improvement.
- The pathway has been missing that mapped a framework from its core elements to specific security controls.
- No guidance is offered for companies on where they should be on the NIST maturity scale: Tier 2? Tier 3? Tier 4?

OPPORTUNITIES

- **Organization integration through merger and acquisition:**
  - *Assess both organizations to understand security risks and priorities prior to integration.*
  - *If the organization is large enough, hire a company to perform an on-site assessment.*
  - *You can quickly get everyone talking the same language and make decisions on risk management.*
- **Evaluate security tool providers and supply chain:**
  - *Know who you’re doing business with and if potential suppliers and partners present a significant risk for accessing or sharing sensitive data.*

THREATS

- Organizations are not able to mitigate cyber security-related liability exposure in the face of regulatory enforcement actions.
- If the organization has a multinational scope, it may opt to pursue an ISO standard to support controls outside of the United States.
- The rigors of framework auditing and enforcement are not understood.

A cyber security framework is a living document. Threats change. Organizations need to be responsive to the changes to remain resilient. Some organizations have a type of compromise, such as data harvesting. A framework helps organize the thoughts into creating a response plan to current situations.

Executive Q&A

Josh Horwitz, COO, Enzoic

ENZOIC

What do security leaders need to know when considering the adoption of cyber standards and frameworks?

There are generally a number of competing standards and frameworks. It is important to benchmark against others in your industry, evaluate the tradeoffs inherent in each and choose the framework that provides the best coverage for your particular business.

How "locked in" is an enterprise when adopting a cyber standard or framework? What have your customers taught you about the decision-making process that you can pass on to organizations looking into this now?

Enterprises are not necessarily "locked in" after choosing a framework; however, change will not be easy. Once a decision is made, the rationale for the initial decision should be documented. If a change is made; there must be a corresponding business justification for the desired change. It is important to avoid standard-hopping just to simplify operations or compliance. It must be rooted in the needs of the business.

What advice do you have for aligning cyber security goals and business objectives?

I believe that all businesses would want to have a solid cyber security posture. When security fails and there is an incident, it puts the business at risk. That said, if security is too burdensome, it may impact the business by limiting its ability to operate quickly, efficiently and to generate sales.

Are there resources to become more informed in making a decision while reducing the risk to the organization?

There are numerous resources to help companies navigate the complexities of compliance. These typically include user groups, trade organizations, online forums and publications. There are also a number of organizations that can come in and help to sort out the details of compliance requirements.

Free resources are available that list known compromised user credentials. What is the value of an on-going service for enterprise security teams?

While free services might meet the needs of some organizations, I think that most organizations would benefit from the types of services offered by Enzoic. First of all, we operate a very sophisticated research function with both human and automated tools that enable us to maintain the most comprehensive database of compromised credentials and passwords available.

Secondly, while free tools often require a lot of manual work, our tools like Enzoic for Active Directory automate detection and remediation of the use of compromised passwords and credentials. Further, in the case of Enzoic for Active Directory, this is a continuous process, which means that we can minimize the attack window during which a compromised credential can be used to compromise a client. Finally, we have great reporting, great tech support and ongoing maintenance.

About Enzoic

Billions of compromised credential and passwords combinations are circulated on the public Internet and Dark Web, putting individuals and organizations at risk. Cybercriminals obtain usernames and passwords from data breaches. Because most people reuse passwords, attackers can then use that data to access accounts on other sites and corporate networks.

Enzoic provides low-friction solutions to detect compromised credentials and prevent attackers from gaining unauthorized access to accounts. It can help organizations prevent targeted, brute force and credential stuffing attacks. Our innovative APIs and Active Directory plugin will check in real-time against billions of exposed username and password combinations, then will alert you of exposure. And all of this is done behind-the-scenes without any unnecessary friction to the user experience.

Organizations can use Enzoic solutions to screen customer and employee accounts for exposed username and password combinations to identity accounts at risk and mitigate unauthorized access.

• *Employee Account Takeover: Enzoic for Active Directory is the only Active Directory plugin to meet NIST 800-63b requirements for real-time blocking of unsafe passwords at set-up and provides continuous monitoring of those same passwords to ensure they don't become vulnerable later. Enzoic for Active Directory enables password policy enforcement and daily exposed password screening to secure passwords in Active Directory. With a fully automated common password screening, fuzzy password matching, password similarity blocking, root password detection, and custom password dictionary filtering; organizations can adopt NIST password requirements with one-click.*

• *Online Customer Account Takeover: Enzoic for Account Takeover is an innovative API solution that allows you to securely compare user credentials against a continuously updated database of compromised credentials. Once an exposure is discovered, you can force a password reset, restrict access or take some other action. This occurs in real-time during user login, account set-up or password reset. Enzoic prevents account takeover fraud with zero false positives and no added friction to the user experience.*

"Despite well-known shortcomings, passwords remain widely used by both consumers as well as enterprise users," said Garrett Bekker, Principal Security Analyst at 451 Research, a unit of S&P Global Market Intelligence. 451 Research's Voice of the Enterprise survey data shows that just 53% of enterprises have deployed multi-factor authentication (MFA), which implies that nearly half of all firms still rely primarily on passwords for authenticating users. Moreover, additional survey data shows that over 71% of users reuse passwords across multiple accounts, which can create significant security risks if those passwords are ever compromised. Enzoic allows enterprises to screen passwords to see if they are common, weak or have been exposed online, which can help organizations strengthen passwords without impacting the user experience.

Enzoic is a privately held company in Colorado.

ENZOIC

To learn more, visit enzoic.com

About Cyber Security Hub

The Cyber Security Hub is an online news source for global cyber security professionals and business leaders who leverage technology and services to secure the entire perimeter in their enterprise.

We're dedicated to providing the latest industry news, thought leadership and analysis in the cyber security space. Cyber Security Hub's expert commentary, tools and resources are developed through obtaining data and interviewing end users and analysts throughout the industry to deliver practical and strategic advice.

Our editorial team surveys and monitors the latest trends in cyber security and creates news articles, market reports, case studies and in-depth analysis for a captive audience consisting of C-Level executives, VPs and directors of cyber security and information technology.

CYBER SECURITY HUB

Dorene Rettas
Managing Director,
Cyber Security Hub
Dorene.Rettas@CSHub.com

Jeff Orr
Editor,
Cyber Security Hub
Jeff.Orr@CSHub.com

Rosecley Morishita
Editorial Director,
Cyber Security Hub
Rosecley.Morishita@iqpc.com

UPCOMING MARKET REPORTS | **MARCH:** Cyber Standards & Industry Frameworks

SOCIAL MEDIA INFORMATION:

Facebook: **CSHubIQPC**

Twitter: **CSHubUSA**

LinkedIn: **Cyber Security Hub - Enterprise Security Professionals**